(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **08335182 A**

(43) Date of publication of application: **17.12.96**

(51) Int. Cl **G06F 12/00**

(21) Application number: **07140497**

(22) Date of filing: **07.06.95**

(71) Applicant: **FUJITSU LTD**

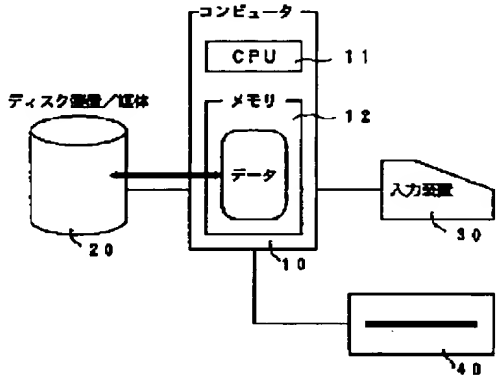
(72) Inventor: **TAKENAKA MASAHIKO**
HASEBE TAKAYUKI
TORII NAOYA
IWAYAMA NOBORU

(54) FILE PROTECTION SYSTEM, SOFTWARE UTILIZATION SYSTEM USING THE SAME AND RECORDING MEDIUM TO BE USED FOR THE SAME

(57) Abstract:

PURPOSE: To prevent the illegal copy of a file by storing information provided by ciphering at a position inside a storage device specified by position information.

CONSTITUTION: When a CD-ROM is set to a CD-ROM driver 40 and the installer of a system software is started, the installer processing of the system software is executed. Concerning this installer processing, first of all, information peculiar for a user system to be used by a user and peculiar equipment information are prepared. Next, the system software is installed in a storage device 20. Concerning the preparation of peculiar equipment information in this case, random numbers are generated, for example, and prescribed numbers are selected out of those random numbers. The prescribed number of digits composed of these selected numbers becomes the peculiar equipment information. Besides, the storage position (address) of the file on the storage device 20 is decided while utilizing those generated random numbers. Thus, since the storage position of the file is decided based on the random numbers, the file is prevented from being stored at the irregular position on the storage device 20 of the user system.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平8－335182

(43)公開日　平成８年(1996)12月17日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　12/00	５３７	7623－5B	Ｇ０６Ｆ　12/00	５３７Ｈ

審査請求　未請求　請求項の数19　ＯＬ　（全 20 頁）

(21)出願番号　特願平7－140497

(22)出願日　平成７年(1995)６月７日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　武仲　正彦
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　長谷部　高行
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(74)代理人　弁理士　伊東　忠彦

最終頁に続く

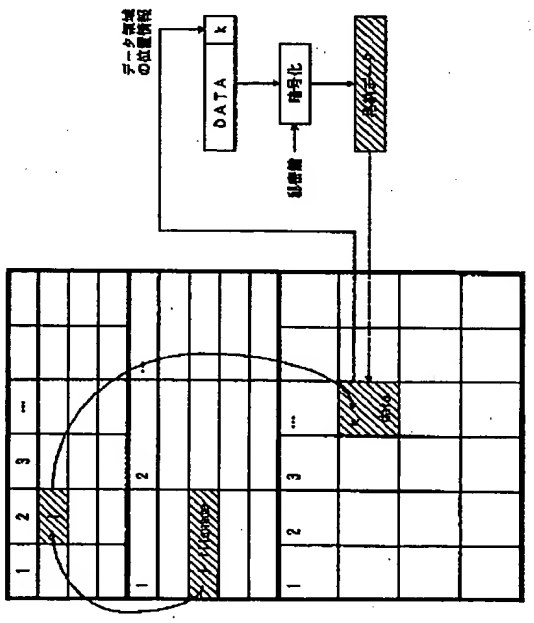
(54)【発明の名称】　ファイル保護システム及びそのファイル保護システムを用いたソフトウエア利用システム及びそのソフトウエア利用システムに用いられる記録媒体

(57)【要約】

【目的】　本発明は、記憶装置に格納されるファイルを保護するためのファイル保護システムにおいて、不正にファイルの移動または複写されたファイルの情報を確実に検出できるようにすることを目的とする。

【構成】　記憶装置に格納されるファイルを保護するためのファイル保護システムにおいて、ファイルの情報を該記憶装置内に格納するために必要な位置情報を決定し、決定された位置情報の少なくとも一部の情報を用いて該ファイルの情報を所定のアルゴリズムに従って暗号化し、該暗号化によって得られた情報を決定された位置情報にて特定される記憶装置内の位置に格納するようにした。

記録装置にファイルの情報を書き込むための処理の例を模式的に示す図



【特許請求の範囲】

【請求項１】　記憶装置に格納されるファイルを保護するためのファイル保護システムにおいて、
ファイルの情報を該記憶装置内に格納するために必要な位置情報を決定する格納位置決定手段と、
該格納位置決定手段にて決定された位置情報の少なくとも一部の情報を用いて該ファイルの情報を所定のアルゴリズムに従って暗号化する暗号化手段とを備え、
該暗号化によって得られた情報を上記格納位置決定手段にて決定された位置情報にて特定される記憶装置内の位置に格納するようにしたファイル保護システム。

【請求項２】　請求項１記載のファイル保護システムにおいて、
上記暗号化手段は、位置情報の少なくとも一部の該情報をファイルの情報に付加する第一の手段と、
該第一の手段にて得られた情報を所定の秘密鍵を用いて暗号化する第二の手段とを有するファイル保護システム。

【請求項３】　請求項１記載のファイル保護システムにおいて、
上記暗号化手段は、位置情報の少なくとも一部の該情報に基づいて秘密鍵を生成する第一の手段と、
該第一の手段にて生成された秘密鍵を用いてファイルの情報を暗号化する第二の手段とを有するファイルの保護システム。

【請求項４】　請求項１記載のファイル保護システムにおいて、
上記暗号化手段は、位置情報の少なくとも一部の該情報をファイルの情報に付加する第一の手段と、
位置情報の少なくとも一部の該情報に基づいて秘密鍵を生成する第二の手段と、
第二の手段にて生成された秘密鍵を用いて該第一の手段にて得られた情報を暗号化する暗号化手段とを有するファイル保護システム。

【請求項５】　請求項１乃至４いずれか記載のファイル保護システムにおいて、
該記憶装置は、ファイルの情報を格納するためのデータ部と、該ファイルの情報が格納されるデータ部内での位置を管理する情報を格納するためのデータ管理部と、ファイル名とそれに対応するデータ管理部内の位置を管理する情報を格納するためのファイル名管理部とを有した論理構造を有すると共に、該格納位置決定手段は、データ部、データ管理部及びファイル名管理部内の各位置をファイルの情報を格納するために必要な位置情報として決定する手段を有し、
該暗号化手段は、データ部、データ管理部及びファイル名管理部の各位置の少なくとも１つに基づいて該ファイルの情報を暗号化するようにしたファイル保護システム。

【請求項６】　請求項１乃至５いずれか記載のファイル保護システムにおいて、
上記格納位置決定手段は、乱数を発生する乱数発生手段を有し、暗号化手段にて用いられる位置情報のうちの少なくとも一部の該情報は乱数発生手段にて得られた乱数に基づいて決定するようにしたファイル保護システム。

【請求項７】　請求項６記載のファイル保護システムにおいて、
上記格納位置決定手段は、乱数にて定まる一又は複数の一時ファイルを所定のアルゴリズムに従って定まる記憶装置内の位置に格納する一時ファイル格納手段と、
該一時ファイル格納手段により一又は複数の一時ファイルが記憶装置に格納された後に、ファイルの情報を格納するために必要な位置情報を該所定のアルゴリズムに従って決定する手段と、
ファイルの情報を格納するために必要な位置情報が決定された後に、上記一時ファイル格納手段にて記憶装置内に格納された一又は複数の一時ファイルを該記憶装置内から削除する手段とを有するファイル保護システム。

【請求項８】　請求項１記載のファイル保護システムによって記憶装置内に格納されたファイルの情報の該記憶装置からの読みだしに関するファイル保護システムにおいて、
記憶装置内の位置を特定する位置情報を指定することにより読みだされたファイルの情報を暗号化手段での暗号化のアルゴリズムに対応したアルゴリズムに従って復合する復合手段と、
復合手段にて得られた情報から暗号化の際に用いられた位置情報の少なくとも一部の該情報を抽出する情報抽出手段と、
該情報抽出手段にて抽出された位置情報の少なくとも一部の該情報と、該ファイルの情報を読みだす際に指定した位置情報の対応する情報とが同一か否かを判定する判定手段とを有し、
該判定手段がそれらの情報が同一でないと判定したときに、復合により得られた該ファイルの情報を正規の情報でないと判定するようにしたファイル保護システム。

【請求項９】　請求項２記載のファイル保護システムによって記憶装置内に格納されたファイルの情報の該記憶装置からの読みだしに関するファイル保護システムにおいて、
記憶装置内の位置を特定する位置情報を指定することにより読みだされたファイルの情報を暗号化手段での暗号化のアルゴリズムに対応したアルゴリズムに従って復合する復合手段と、
復合手段にて得られた情報から該ファイルの情報及び該情報に付加された位置情報の少なくとも一部の該情報を分離する情報分離手段と、
該情報分離手段にて得られた位置情報の少なくとも一部の該情報と、該ファイルの情報を読みだす再に指定した位置情報の対応する情報とが同一か否かを判定する判定

手段とを有し、
該判定手段がそれらの情報が同一でないと判定したときに、復合により得られた該ファイルの情報を正規の情報でないと判定するようにしたファイル保護システム。
【請求項１０】　請求項３記載のファイル保護システムによって記憶装置内に格納されたファイルの情報の該記憶装置からの読みだしに関するファイル保護システムにおいて、
記憶装置内の位置を特定する位置情報を指定して該ファイルの情報を読みだす際に、該位置情報のうち、上記暗号化手段にて用いられた位置情報の少なくとも一部の該情報に対応した情報に基づいて秘密鍵を生成する秘密鍵生成手段と、
該秘密鍵生成手段にて生成された秘密鍵を用いて該記憶装置内より読みだされた情報を復合する復合手段とを有するファイルの保護システム。
【請求項１１】　請求項４記載のファイル保護システムによって記憶装置内に格納されたファイルの情報の該記憶装置からの読みだしに関するファイルの保護システムにおいて、
記憶装置内の位置を特定する位置情報を指定して該ファイルの情報を読みだす際に、該位置情報のうち、上記暗号化手段にて用いられた位置情報の少なくとも一部の該情報に対応した情報に基づいて秘密鍵を生成する秘密鍵生成手段と、
該秘密鍵生成手段にて生成された秘密鍵を用いて該記憶装置内より読みだされた情報を復合する復合手段と、
該復合手段にて得られた情報から該ファイルの情報及び該情報に付加された位置情報の少なくとも一部の該情報を分離する情報分離手段と、
該情報分離手段にて得られた位置情報の少なくとも一部の該情報と、該ファイルの情報を読みだす際に指定した位置情報の対応する情報とが同一か否かを判定する判定手段とを有し、
該判定手段がそれらの情報が同一でないと判定したときに、復合により得られた該ファイルの情報を正規の情報でないと判定するようにしたファイル保護システム。
【請求項１２】　指定された位置情報に情報が格納される記憶装置と、
当該ソフトウエア利用システムを特定する固有情報を該記憶装置内に格納するために必要な位置情報を決定する格納位置決定手段と、
該格納位置決定手段にて決定された位置情報の少なくとも一部の情報を用いて該固有情報を所定のアルゴリズムに従って暗号化する暗号化手段と、
該暗号化によって得られた情報を上記格納位置決定手段にて決定された位置情報にて特定される記憶装置内の位置に格納する情報格納制御手段と、
該記憶装置内の位置を特定する位置情報を指定することにより読みだされた該暗号化された情報を上記暗号化手段での暗号化のアルゴリズムに対応したアルゴリズムに従って復合する第一の復合手段と、
第一の復合手段にて得られた情報から暗号化の際に用いられた位置情報の少なくとも一部の該情報及び固有情報を抽出する情報抽出手段と、
該情報抽出手段にて抽出された位置情報の少なくとも一部の該情報と、該暗号化された情報を読みだす際に指定した位置情報の対応する情報とが同一か否かを判定する判定手段と、
該判定手段がそれらの情報が同一である判定したときに、外部のシステムから供給される暗号化されたソフトウエアを復合するための鍵であって上記固有情報にて暗号化された鍵を該情報抽出手段にて抽出された固有情報を用いて復合する第二の復合手段と、
該第二の復合手段にて得られた鍵を用いて、上記外部から供給される暗号化されたソフトウエアを復合する第三の復合手段とを有するソフトウエア利用システム。
【請求項１３】　請求項１２記載のソフトウエア利用システムにおいて、
該暗号化手段は、位置情報の少なくとも一部の該情報を該固有情報に付加する第一の手段と、
該第一の手段にて得られた情報を所定の秘密鍵を用いて暗号化する第二の手段とを有するソフトウエア利用システム。
【請求項１４】　指定された位置情報に情報が格納される記憶装置と、
当該ソフトウエア利用システムを特定する固有情報を該記憶装置内に格納するために必要な位置情報を決定する格納位置決定手段と、
該格納位置決定手段にて決定された位置情報の少なくとも一部の情報に基づいて秘密鍵を生成する第一の秘密鍵生成手段と、
該第一の秘密鍵生成手段にて生成された秘密鍵を用いて該固有情報を暗号化する暗号化手段と、
該暗号化によって得られた情報を上記格納位置決定手段にて決定された位置情報にて特定される記憶装置内の位置に格納する情報格納制御手段と、
記憶装置内の位置を特定する位置情報を指定して該暗号化された固有情報を読みだす際に、該位置情報のうち、上記暗号化手段にて用いられた位置情報の少なくとも一部の該情報に対応した情報に基づいて秘密鍵を生成する第二の秘密鍵生成手段と、
該第二の秘密鍵生成手段にて生成された秘密鍵を用いて該記憶装置内より読みだされた情報を復合して固有情報を得るための第一の復合手段と、
外部のシステムから供給される暗号化されたソフトウエアを復合するための鍵であって上記固有情報にて暗号化された鍵を該第一の復合手段にて得られた固有情報を用いて復合する第二の復合手段と該第二の復合手段にて得られた鍵を用いて、上記外部から供給される暗号化され

たソフトウエアを復合する第三の復合手段とを有するソフトウエア利用システム。

【請求項１５】　指定された位置情報に情報が格納される記憶装置と、
当該ソフトウエア利用システムを特定する固有情報を該記憶装置内に格納するために必要な位置情報を決定する格納位置決定手段と、
該格納位置決定手段にて決定された位置情報の少なくとも一部の情報をファイルの情報に付加する情報付加手段と、
位置情報の少なくとも一部の該情報に基づいて秘密鍵を生成する第一の秘密鍵生成手段と、
該第一の秘密鍵生成手段にて生成された秘密鍵を用いて該情報付加手段にて得られた情報を暗号化する暗号化手段と、
該暗号化によって得られた情報を上記格納位置決定手段にて決定された位置情報にて特定される記憶装置内の位置に格納する情報格納制御手段と、
記憶装置内の位置を特定する位置情報を指定して該暗号化された固有情報を読みだす際に、該位置情報のうち、上記暗号化手段にて用いられた位置情報の少なくとも一部の該情報に対応した情報に基づいて秘密鍵を生成する第二の秘密鍵生成手段と、
該第二の秘密鍵生成手段にて生成された秘密鍵を用いて該記憶装置内より読みだされた情報を復合する第一の復合手段と、
該第一の復合手段にて得られた情報から該固有情報及び該固有情報に付加された位置情報の少なくとも一部の該情報を分離して抽出する情報抽出手段と、
該情報抽出手段にて得られた位置情報の少なくとも一部の該情報と、該ファイルの情報を読みだす際に指定した位置情報の対応する情報とが同一か否かを判定する判定手段と、
該判定手段がそれらの情報が同一である判定したときに、外部のシステムから供給される暗号化されたソフトウエアを復合するための鍵であって上記固有情報にて暗号化された鍵を該情報抽出手段にて抽出された固有情報を用いて復合する第二の復合手段と、
該第二の復合手段にて得られた鍵を用いて、上記外部から供給される暗号化されたソフトウエアを復合する第三の復合手段とを有するソフトウエア利用システム。

【請求項１６】　請求項１２乃至１５いずれか記載のソフトウエア利用システムにおいて、更に、記憶装置に格納されるべき固有情報を生成する固有情報生成手段を備えたソフトウエア利用システム。

【請求項１７】　請求項１６記載のソフトウエア利用システムにおいて、該固有情報生成手段は、乱数を発生する乱数発生手段を有し、該乱数発生手段にて発生される乱数に基づいて該固有情報を生成するようにしたソフトウエア利用システム。

【請求項１８】　請求項１２乃至１７いずれか記載のソフトウエア利用システムにおいて、該ソフトウエア利用システム内にて利用されるソフトウエアは、外部から供給される記録媒体に暗号化された状態で格納されており、更に、暗号化された該ソフトウエアを該記録媒体から読みだす手段を備えたソフトウエア利用システム。

【請求項１９】　請求項１８記載のソフトウエア利用システムに用いられる記録媒体であって、
当該ソフトウエア利用システムにて利用可能な暗号化されたソフトウエアと該暗号化されたソフトウエアを該ソフトウエア利用システムに読みだすために必要な情報とが記録された領域と、
当該ソフトウエア利用システムの記憶装置に格納すべき該固有情報を発生させるために必要な情報を格納した領域を有する記録媒体。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、コンピュータシステムにて用いられる各種情報（ファイル）の不正利用を防止するファイル保護システム及びその保護システムを用いたソフトウエアの利用システム及びそのソフトウエア利用システムに用いられる記録媒体に係り、詳しくは、ファイルの他のコンピュータシステムへの移動や複写、改ざんを確実に検出できるようにしたファイル保護システム更にそのファイル保護システムを用いてソフトウエアが正規のユーザにのみ利用可能となるソフトウエア利用システム、更にまたそのソフトウエア利用システムに用いられる記録媒体に関する。

【０００２】

【従来の技術】近年、ソフトウエアが保護された状態で格納されたＣＤ－ＲＯＭや光磁気ディスク（ＭＯ）等の記録媒体と、その記録媒体内のソフトウエアの保護状態を解除するためのライセンス（鍵）を別々に販売するソフトウエアの販売形態が提案されている。具体的には、図２３に示すように、あるソフトウエア（アプリケーション等）（以下ソフト１という）が錠１１０がかけられた状態（暗号化された状態）で格納されたＣＤ－ＲＯＭ１００と、このソフト１の錠１１０をあけるための鍵１２０（ライセンス）を別々に、例えばユーザＡが購入する。この鍵１２０（ライセンス）は更にユーザ固有の錠１２１がかけられてた状態（暗号化された状態）でユーザＡに渡される。ソフトウエアを利用するユーザＡのシステム２００に格納されたユーザＡ固有（システム２００固有）の鍵２１０によってこの錠１２１が解除される（復合）ようになっている。その結果、ユーザＡのソフトウエア利用システム２００に錠１１０のついた状態でインストールされたソフト１は、ユーザＡ固有の鍵２１０及びソフト１の鍵１１０によってその錠１１０が解除され（復合され）、ユーザＡのシステム２００において使用可能な状態となる。

【０００３】このように保護された状態でＣＤ－ＲＯＭ１００に格納されたソフト１は、ユーザＢが仮にソフト１の鍵１２０を入手しても、ユーザＢはユーザＢ固有の鍵３１０は持ちうるが、ユーザＡ固有の鍵２１０をもっていないので、ユーザＢのソフトウエア利用システム３００においては利用することができない。

【０００４】

【発明が解決しようとする課題】しかし、上記のようなファイル（ソフトウエア等）の保護システムでは、ユーザＡのシステム２００に格納されたユーザＡ固有の鍵２１０及びソフト１の鍵１２０を他のシステムにコピーした場合、その他のシステムにインストールされたソフト１は、当該他のシステムにて利用できてしまう。

【０００５】そこで、本発明の第一の目的は、上記ユーザＡ固有の鍵の入ったファイル等、秘密にすべきファイルを他のシステムに不正に複写することを防止するファイル保護システムを提供することである。また、本発明の第二の目的は、このファイル保護システムを用いたソフトウエア利用システムを提供することである。

【０００６】更にまた、本発明の第三の目的は、このソフトウエア利用システムにて用いられる記録媒体を提供することである。

【０００７】

【課題を解決するための手段】上記第一の目的を達成するため、本発明は、請求項１に記載されるように、記憶装置に格納されるファイルを保護するためのファイル保護システムにおいて、ファイルの情報を該記憶装置内に格納するために必要な位置情報を決定する格納位置決定手段と、該格納位置決定手段にて決定された位置情報の少なくとも一部の情報を用いて該ファイルの情報を所定のアルゴリズムに従って暗号化する暗号化手段とを備え、該暗号化によって得られた情報を上記格納位置決定手段にて決定された位置情報にて特定される記憶装置内の位置に格納するようにした。

【０００８】該ファイル保護システムにおいて、該暗号化手段を具体化する観点から、請求項２に記載されるように、上記暗号化手段は、位置情報の少なくとも一部の該情報をファイルの情報に付加する第一の手段と、該第一の手段にて得られた情報を所定の秘密鍵を用いて暗号化する第二の手段とを有するようにした。

【０００９】また、同観点から、請求項３に記載されるように、上記暗号化手段は、位置情報の少なくとも一部の該情報に基づいて秘密鍵を生成する第一の手段と、該第一の手段にて生成された秘密鍵を用いてファイルの情報を暗号化する第二の手段とを有するようにした。

【００１０】更に同観点から、請求項４に記載されるように、上記暗号化手段は、位置情報の少なくとも一部の該情報をファイルの情報に付加する第一の手段と、位置情報の少なくとも一部の該情報に基づいて秘密鍵を生成する第二の手段と、第二の手段にて生成された秘密鍵を用いて該第一の手段にて得られた情報を暗号化する暗号化手段とを有するようにした。

【００１１】また、上記ファイル保護システムにおいて、情報の格納位置をランダムに決定できるという観点から、請求項６に記載されるように、上記格納位置決定手段は、乱数を発生する乱数発生手段を有し、暗号化手段にて用いられる位置情報のうちの少なくとも一部の該情報は乱数発生手段にて得られた乱数に基づいて決定するようにした。

【００１２】請求項１に記載されるファイル保護システムによって記憶装置内に格納されたファイルの情報の該記憶装置からの読みだしに関するファイル保護システムを提供するという観点から、請求項８に記載されるように、記憶装置内の位置を特定する位置情報を指定することにより読みだされたファイルの情報を暗号化手段での暗号化のアルゴリズムに対応したアルゴリズムに従って復合する復合手段と、復合手段にて得られた情報から暗号化の際に用いられた位置情報の少なくとも一部の該情報を抽出する情報抽出手段と、該情報抽出手段にて抽出された位置情報の少なくとも一部の該情報と、該ファイルの情報を読みだす際に指定した位置情報の対応する情報とが同一か否かを判定する判定手段とを有し、該判定手段がそれらの情報が同一でないと判定したときに、復合により得られた該ファイルの情報を正規の情報でないと判定するようにした。

【００１３】また、請求項２に記載されるファイル保護システムによって記憶装置内に格納されたファイルの情報の該記憶装置からの読みだしに関するファイル保護システムを提供するという観点から、請求項９に記載されるように、記憶装置内の位置を特定する位置情報を指定することにより読みだされたファイルの情報を暗号化手段での暗号化のアルゴリズムに対応したアルゴリズムに従って復合する復合手段と、復合手段にて得られた情報から該ファイルの情報及び該情報に付加された位置情報の少なくとも一部の該情報を分離する情報分離手段と、該情報分離手段にて得られた位置情報の少なくとも一部の該情報と、該ファイルの情報を読みだす際に指定した位置情報の対応する情報とが同一か否かを判定する判定手段とを有し、該判定手段がそれらの情報が同一でないと判定したときに、復合により得られた該ファイルの情報を正規の情報でないと判定するようにした。

【００１４】更にまた、請求項３に記載されるファイル保護システムによって記憶装置内に格納されたファイルの情報の該記憶装置からの読みだしに関するファイル保護システムを提供するという観点から、請求項１０に記載されるように、記憶装置内の位置を特定する位置情報を指定して該ファイルの情報を読みだす際に、該位置情報のうち、上記暗号化手段にて用いられた位置情報の少なくとも一部の該情報に対応した情報に基づいて秘密鍵を生成する秘密鍵生成手段と、該秘密鍵生成手段にて生

成された秘密鍵を用いて該記憶装置内より読みだされた情報を復合する復合手段とを有するようにした。

【００１５】また、、請求項４に記載されるファイル保護システムによって記憶装置内に格納されたファイルの情報の該記憶装置からの読みだしに関するファイル保護システムを提供するという観点から、請求項１１に記載されるように、記憶装置内の位置を特定する位置情報を指定して該ファイルの情報を読みだす際に、該位置情報のうち、上記暗号化手段にて用いられた位置情報の少なくとも一部の該情報に対応した情報に基づいて秘密鍵を生成する秘密鍵生成手段と、該秘密鍵生成手段にて生成された秘密鍵を用いて該記憶装置内より読みだされた情報を復合する復合手段と、該復合手段にて得られた情報から該ファイルの情報及び該情報に付加された位置情報の少なくとも一部の該情報を分離する情報分離手段と、該情報分離手段にて得られた位置情報の少なくとも一部の該情報と、該ファイルの情報を読みだす際に指定した位置情報の対応する情報とが同一か否かを判定する判定手段とを有し、該判定手段がそれらの情報が同一でないと判定したときに、復合により得られた該ファイルの情報を正規の情報でないと判定するようにした。

【００１６】上記第二の目的を達成するため、本発明は、請求項１２に記載されるように、指定された位置情報に情報が格納される記憶装置と、当該ソフトウエア利用システムを特定する固有情報を該記憶装置内に格納するために必要な位置情報を決定する格納位置決定手段と、該格納位置決定手段にて決定された位置情報の少なくとも一部の情報を用いて該固有情報を所定のアルゴリズムに従って暗号化する暗号化手段と、該暗号化によって得られた情報を上記格納位置決定手段にて決定された位置情報にて特定される記憶装置内の位置に格納する情報格納制御手段と、該記憶装置内の位置を特定する位置情報を指定することにより読みだされた該暗号化された情報を上記暗号化手段での暗号化のアルゴリズムに対応したアルゴリズムに従って復合する第一の復合手段と、第一の復合手段にて得られた情報から暗号化の際に用いられた位置情報の少なくとも一部の該情報及び固有情報を抽出する情報抽出手段と、該情報抽出手段にて抽出された位置情報の少なくとも一部の該情報と、該暗号化された情報を読みだす際に指定した位置情報の対応する情報とが同一か否かを判定する判定手段と、該判定手段がそれらの情報が同一である判定したときに、外部のシステムから供給される暗号化されたソフトウエアを復合するための鍵であって上記固有情報にて暗号化された鍵を該情報抽出手段にて抽出された固有情報を用いて復合する第二の復合手段と、該第二の復合手段にて得られた鍵を用いて、上記外部から供給される暗号化されたソフトウエアを復合する第三の復合手段とを有するようにした。

【００１７】また、上記第二の目的を達成するため、本発明は、請求項１４に記載されるように、当該ソフトウエア利用システムを特定する固有情報を該記憶装置内に格納するために必要な位置情報を決定する格納位置決定手段と、該格納位置決定手段にて決定された位置情報の少なくとも一部の情報に基づいて秘密鍵を生成する第一の秘密鍵生成手段と、該第一の秘密鍵生成手段にて生成された秘密鍵を用いて該固有情報を暗号化する暗号化手段と、該暗号化によって得られた情報を上記格納位置決定手段にて決定された位置情報にて特定される記憶装置内の位置に格納する情報格納制御手段と、記憶装置内の位置を特定する位置情報を指定して該暗号化された固有情報を読みだす際に、該位置情報のうち、上記暗号化手段にて用いられた位置情報の少なくとも一部の該情報に対応した情報に基づいて秘密鍵を生成する第二の秘密鍵生成手段と、該第二の秘密鍵生成手段にて生成された秘密鍵を用いて該記憶装置内より読みだされた情報を復合して固有情報を得るための第一の復合手段と、外部のシステムから供給される暗号化されたソフトウエアを復合するための鍵であって上記固有情報にて暗号化された鍵を該第一の復合手段にて得られた固有情報を用いて復合する第二の復合手段と、該第二の復合手段にて得られた鍵を用いて上記外部から供給される暗号化されたソフトウエアを復合する第三の復合手段とを有するようにした。

【００１８】更にまた、上記第二の目的を達成するため、本発明は、請求項１５に記載されるように、指定された位置情報に情報が格納される記憶装置と、当該ソフトウエア利用システムを特定する固有情報を該記憶装置内に格納するために必要な位置情報を決定する格納位置決定手段と、該格納位置決定手段にて決定された位置情報の少なくとも一部の情報をファイルの情報に付加する情報付加手段と、位置情報の少なくとも一部の該情報に基づいて秘密鍵を生成する第一の秘密鍵生成手段と、該第一の秘密鍵生成手段にて生成された秘密鍵を用いて該情報付加手段にて得られた情報を暗号化する暗号化手段と、該暗号化によって得られた情報を上記格納位置決定手段にて決定された位置情報にて特定される記憶装置内の位置に格納する情報格納制御手段と、記憶装置内の位置を特定する位置情報を指定して該暗号化された固有情報を読みだす際に、該位置情報のうち、上記暗号化手段にて用いられた位置情報の少なくとも一部の該情報に対応した情報に基づいて秘密鍵を生成する第二の秘密鍵生成手段と、該第二の秘密鍵生成手段にて生成された秘密鍵を用いて該記憶装置内より読みだされた情報を復合する第一の復合手段と、該第一の復合手段にて得られた情報から該固有情報及び該固有情報に付加された位置情報の少なくとも一部の該情報を分離して抽出する情報抽出手段と、該情報抽出手段にて得られた位置情報の少なくとも一部の該情報と、該ファイルの情報を読みだす際に指定した位置情報の対応する情報とが同一か否かを判定

する判定手段と、該判定手段がそれらの情報が同一である判定したときに、外部のシステムから供給される暗号化されたソフトウエアを復合するための鍵であって上記固有情報にて暗号化された鍵を該情報抽出手段にて抽出された固有情報を用いて復合する第二の復合手段と、該第二の復合手段にて得られた鍵を用いて、上記外部から供給される暗号化されたソフトウエアを復合する第三の復合手段とを有するようにした。

【００１９】機体番号等のシステム固有の情報を予め備えていないシステムであっても当該ソフトウエア利用システムが実現できるという観点から、請求項１６に記載されるように、上記ソフトウエア利用システムにおいて、更に、記憶装置に格納されるべき固有情報を生成する固有情報生成手段を備えるようにした。

【００２０】このソフトウエア利用システムにおいて、システムの固有情報を容易に生成できるどいう観点から、請求項１７に記載されるように、該固有情報生成手段は、乱数を発生する乱数発生手段を有し、該乱数発生手段にて発生される乱数に基づいて該固有情報を生成するようにした。

【００２１】該ソフトウエア利用システムに対して容易にソフトウエアを供給できるという観点から、請求項１８に記載されるように、上記各ソフトウエア利用システムにおいて、該ソフトウエア利用システム内にて利用されるソフトウエアは、外部から供給される記録媒体に暗号化された状態で格納されており、更に、暗号化された該ソフトウエアを該記録媒体から読みだす手段を備えるようにした。

【００２２】上記第三の目的を達成するため、本発明は、請求項１９に記載されるように、上記ソフトウエア利用システムにソフトウエアを提供するための記録媒体において、当該ソフトウエア利用システムにて利用可能な暗号化されたソフトウエアと該暗号化されたソフトウエアを該ソフトウエア利用システムに読みだすために必要な情報とが記録された領域と、当該ソフトウエア利用システムの記憶装置に格納すべき該固有情報を発生させるために必要な情報を格納した領域を有するようにした。

【００２３】

【作用】請求項１、２及び４記載のファイル保護システムでは、ファイルを格納すべき記憶装置内の位置情報の少なくとも一部の情報に基づいてファイルの情報が暗号化され、その暗号化された情報が記憶装置のその位置情報にて特定される位置に格納される。従って、該ファイルの情報を他のシステムに複写した場合、当該他のシステムにおける複写位置と該暗号化に用いられた位置の情報の差に基づいて、当該ファイルの情報が複写されたことが検出できる。

【００２４】即ち、請求項８、９及び１１に記載されるファイル保護システムでは、記憶装置から読みだされた暗号化された情報が復合され、復合にて得られた情報から暗号化の際に用いられた位置情報の少なくとも一部の該情報が抽出され、その抽出された位置情報の少なくとも一部の該情報と、該ファイルの情報を読みだす際に指定した位置情報の対応する情報とが同一か否かが判定される。それらの情報が同一でないと判定したときに、復合により得られた該ファイルの情報は正規の情報でないと判定される。

【００２５】請求項３及び４記載のファイル保護システムでは、ファイルを格納すべき記憶装置内の位置情報の少なくとも一部に基づいて秘密鍵が生成され、その秘密鍵を用いて記憶装置に格納すべきファイルの情報が暗号化される。従って、該ファイルの情報を他のシステムに複写した場合、当該他のシステムにおいて、秘密鍵の生成の基礎となる記憶位置に関する情報がわからないので、このファイルの情報を復合することができない。

【００２６】請求項１０及び１１に記載されるファイル保護システムでは、記憶装置内の位置を特定する位置情報を指定して該ファイルの情報を読みだす際に、該位置情報のうち、上記暗号化にて用いられた位置情報の少なくとも一部の該情報に対応した情報に基づいて秘密鍵が生成され、該生成された秘密鍵を用いて該記憶装置内より読みだされた情報が復合される。その復合の結果、記憶装置に格納されたファイルの情報が再現される。

【００２７】請求項１２、１４及び１５記載のソフトウエア利用システムでは、当該システムの固有情報が上述したファイル保護システムにて保護された状態で記憶装置内に格納されると共に記憶装置内から読みだされる。そして、この固有情報にて暗号化された鍵が記憶装置から読みだされた該固有情報を用いて復合する。暗号化された状態で外部から供給されるソフトウエアが、上記復合された鍵を用いて復合される。

【００２８】請求項１９記載の記録媒体は、上述したソフトウエア利用システムにセットされる。その状態で、固有情報を発生させるために必要な情報を用いて該固有情報が発生させられる。そして、該固有情報が上述したファイル保護システムにて保護された状態で記憶装置に格納される。また、暗号化されたソフトウエアがソフトウエア利用システムに読みだすために必要な情報を用いて読みだされ、暗号化された該ソフトウエアが該ソフトウエア利用システムに提供される。

【００２９】

【実施例】以下、本発明の実施例を図面に基づいて説明する。図１は、本発明の実施例に係るファイル保護システムが適用されるユーザシステム（コンピュータシステム）の基本構成図である。

【００３０】図１において、このユーザシステムは、基本的に、コンピュータユニット１０、記憶装置２０、入力装置３０及びＣＤ－ＲＯＭドライバ４０を有している。記憶装置２０はディスク装置等で構成され、保護の

対象となるファイル（秘密のデータ等）が格納される。コンピュータユニット１０は、各種処理の制御を行うＣＰＵ１１と記憶装置２０から読みだしたファイルを格納するメモリ１２とを備えている。コンピュータユニット１０のＣＰＵ１１は入力装置３０からのユーザ操作に基づいた情報に従ってメモリ１２内のデータ等を処理する。また、ＣＤ－ＲＯＭドライバ４０にセットされたＣＤ－ＲＯＭから所望のソフトウエア（アプリケーション等）が読みだされて、記憶装置２０にインストールされる。

【００３１】図１に示すようなユーザシステムのユーザは、図２に示すように、複数のソフト（アプリケーション等）及びシステムソフトが格納された、記録媒体、例えば、ＣＤ－ＲＯＭを購入する。各ソフト及びシステムソフトは、そのインストーラと共に錠がかけられた状態（暗号化された状態）でＣＤ－ＲＯＭに格納されている。このＣＤ－ＲＯＭを購入したユーザは、図３に示す手順に従って、所望のソフトを自らのユーザシステムにインストールするための作業を行う。図３において、まず、ＣＤ－ＲＯＭ内のシステムソフトの当該ユーザシステムへのインストールを行い、ＣＤ－ＲＯＭに保護状態（暗号化された状態）で格納された所望のソフトｉの鍵（ライセンス）を購入する（Ｓ２）。その後、ＣＤ－ＲＯＭから該所望のソフトｉを当該ユーザシステムにインストールし（Ｓ３）、購入した鍵（ライセンス）によって該ソフトｉの保護状態を解除（復合）してそのソフトｉを図１に示すようなユーザシステム内で実行する（Ｓ４）。

【００３２】上記のユーザの作業手順において、システムソフトのインストールは、図４に示すように行われる。即ち、図２に示すようなＣＤ－ＲＯＭをＣＤ－ＲＯＭドライバ４０にセットし、システムソフトのインストーラを起動させると、システムソフトのインストーラ処理が実行される。このインストーラ処理では、まず、当該ユーザが使用する図１に示すようなユーザシステム固有の情報、機器固有情報を作成する（Ｓ１１）。次いで、システムソフトを記憶装置２０内にインストールする（Ｓ１２）。

【００３３】上記機器固有情報の作成は、例えば、図５に示す手順に従って行われる。図５において、乱数を発生させ、その乱数から所定の数を選択する（Ｓ１１１）。この選択された数により構成される所定桁数の数が機器固有情報となる。また、その発生した乱数を利用して、記憶装置２０上でのファイルの格納位置（アドレス）を決める（Ｓ１１２）。このように、乱数に基づいてファイルの格納位置を決定することにより、ユーザシステムの記憶装置２０上の不規則な位置にファイルが格納されることになる。

【００３４】ところで、記憶装置２０の論理構造は、例えば、図６に示すようになっている。即ち、記憶装置２０は、データ部、ファイル名管理部及びデータ管理部に分割されている。データ部はファイルのデータを格納し、データ管理部はデータの格納位置を管理し、また、ファイル名管理部はファイル名とデータ管理部との関係を管理している。

【００３５】上記のように、記憶装置２０上でのファイルの格納位置が決定されると、図５におけるステップＳ１１３以降のような手順に従って処理が行われる。この処理は、図７に模式的に示される。図７を参照して図５におけるステップＳ１１３以降の処理を説明する。

【００３６】まず、機器固有情報を書き込むためのファイルがオープンされる（Ｓ１１３）。記憶装置２０のデータ部、ファイル名管理部、データ管理部のそれぞれに、上記のように決定された該ファイルを格納するために必要な領域の位置情報ｋ，ｊ，ｉが割り付けられる。そして、データ部に割り付けられた領域の位置情報ｋが付加データとして獲得される（Ｓ１１４）。データ部の該領域の位置情報ｋが獲得されると、格納すべきデータDATA（機器固有情報）に該位置情報ｋが付加される（Ｓ１１５）。そして、このデータDATAと位置情報ｋが一体となったデータ（DATA+k）が予め当該ユーザシステムに与えられた秘密鍵を用いて暗号化され、暗号化データEkey(DATA+k)が生成される（Ｓ１１６）。この暗号化データが該位置情報ｋにて特定されるデータ部の領域に書き込まれる（Ｓ１１７）。その後、該データ（機器固有情報）に関する他の必要情報が位置情報ｉ，ｊで特定されるデータ管理部及びファイル名管理部の各領域に書き込まれる。そして、全ての情報の書込が完了した後に、ファイルがクローズされる（Ｓ１１８）。

【００３７】次に、所望のソフトの保護状態を解除するための鍵（ライセンス）の購入は、図８に示す手順に従って、ユーザシステムにおいて行われる。図８において、まず上記のように暗号化して記憶装置２０に格納された機器固有情報を記憶装置２０から読みだして復合する（Ｓ２１）。この機器固有情報の読みだし処理の詳細は後述する。その後、所望のソフトｉを特定する情報（ＩＤ番号等）と機器固有情報に対応した鍵購入用番号とを電子メール、電話等を利用してソフトの鍵（ライセンス）を販売するセンタに通知する（Ｓ２２）。通知を受けたセンタは、ユーザが希望するソフトの錠（暗号化された）を解除するための（復合するための）鍵（ライセンス）を機器固有情報に対応した鍵購入用番号を用いて暗号化する（錠をかける）。そして、その錠がかけられた鍵（ライセンス）を電話等を利用してユーザに通知する。その通知を受けたユーザは、入力装置３０を用いてユーザシステム内に該暗号化された鍵（ライセンス）を入力する（Ｓ２３）。すると、その暗号化された鍵（ライセンス）が記憶装置２０の所定の領域に格納される（Ｓ２４）。

【００３８】上記機器固有情報の読みだし処理（Ｓ２

１）は、次のように行われる。保護されたファイルのデータを記憶装置２０から読み出す場合、コンピュータユニット１０は図１０に示す手順に従って機器固有情報の読みだし処理を実行する。この図１０に示す処理の手順が図９に模式的に示される。図９及び図１０を参照して機器固有情報の読出処理について説明する。

【００３９】機器固有情報のファイルがオープンされると（Ｓ２１１）、該ファイルのファイル名に基づいて記憶装置２０上でのデータ管理部、ファイル名管理部及びデータ部のそれぞれにおけるファイルに関する情報の格納領域の位置情報ｉ’、ｊ’、ｋ’が特定される。そして、暗号化データEkey(DATA+k)（暗号化された機器固有情報及び位置情報）が格納された領域の位置情報ｋ’が獲得される（Ｓ２１２）。また、暗号化データEkey(DATA+k)が記憶装置２０のこの位置情報ｋ’にて特定される領域から読みだされる（Ｓ２１３）。この読みだされた暗号化データEkey(DATA+k)はコンピュータユニット１０の、メモリ１２に格納される。その後、メモリ１２内の暗号化データEkey(DATA+k)が秘密鍵を用いて復合され（Ｓ２１４）、元のデータDATA（機器固有情報）と付加データとしての位置情報ｋが分離される（Ｓ２１５）。このようにして得られた位置情報ｋと該暗号化データが格納されていた領域の位置情報ｋ’とが比較され、それらが同一であるか否かが判定される（Ｓ２１６）。ここで、それらの位置情報ｋ及びｋ’が同一であれば、この機器固有情報に関するファイルは移動、複写等されていないので、正常な処理としてファイルがクローズされる（Ｓ２１７）。この場合、ステップＳ２１４にて復合された機器固有情報が当該ユーザシステムにて利用される。即ち、この機器固有情報が希望するソフトの錠を解く鍵（ライセンス）を購入するためにセンタに通知される（図８参照）。

【００４０】一方、上記各位置情報ｋ及びｋ’が同一でない場合、機器固有情報に関するファイルは移動あるいは複写されたものとしてエラー信号が出力される。この場合、エラー信号に基づいて、例えば、読みだしたデータの処理が強制的に中断される。

【００４１】上記のように、本実施例では、各ユーザシステムの使用環境に応じてファイルの格納位置が異なることを利用して機器固有情報に関するファイルの不正な移動あるいは複写が検出される。上記のようにして、ユーザが希望したソフトの錠（保護状態）を解くための鍵（ライセンス）をセンタから購入した後に、ユーザは、その鍵（ライセンス）を用いて、図１に示すようなＣＤ－ＲＯＭに保護状態となって（暗号化されて）格納された所望のソフトをユーザシステムにインストールするための処理を行う。このソフトのインストールは、図１１に示す手順に従って行われる。

【００４２】図１１において、まず、機器固有情報を読みだす（Ｓ３１）。この処理は、図９及び図１０に従って説明したのと同様に行われる。即ち、暗号化された機器固有情報DATAと位置情報ｉが復合され、その復合された位置情報ｉと実際に読みだした記憶装置２０上の位置を表わす位置情報ｉ’とが同一か否かを判定する。そして、同一でなければ、この暗号化された位置情報が不正に複写されたものと判定して、エラー信号を出力して以後の処理を中断する。一方、上記各位置情報ｉ及びｉ’が同一であれば、復合された機器固有情報を用いて以後の処理が継続される。

【００４３】暗号化された鍵（ライセンス）が記憶装置２０の所定の領域から読みだされ、その暗号化された鍵（ライセンス）が上記のようにして読みだされた機器固有情報を用いて復合される（Ｓ３２）。この復合により得られた鍵（ライセンス）を用いて更に、保護状態（錠がかけられた状態）ソフトの開錠処理（復合）が行われる（Ｓ３３）。そして、保護状態がとかれたソフトが記憶装置２０内にインストールされる。ここで、例えば、鍵（ライセンス）と関係の無いソフトのインストールを行おうとした場合、上記開錠処理が正常に行われず、エラー信号が出力され、以後の処理が中断される。

【００４４】ライセンスの購入の際の処理と同様に、機器固有情報が、その各ユーザシステム固有の格納位置情報に基づいて保護されているので、機器固有情報を複写したユーザシステムでは、錠がかけられた状態（保護状態）のソフトを解くための（復合するための）鍵（ライセンス）を得ることはできない。従って、図１に示すようなＣＤ－ＲＯＭにてユーザに供給された各ソフト（アプリケーション等）が高い安全性をもって保護される。

【００４５】次に、機器固有情報の格納及び読みだしに関する他の処理例を図１２乃至図１５に基づいて説明する。保護すべき機器固有情報に関するファイルを記憶装置２０に格納する場合、コンピュータユニット１０はその格納処理の一部として、図１４に示すような処理を実行する。この図１４に示す処理の手順が図１２に模式的に示される。

【００４６】この場合、上述したデータ書込時の処理（図５参照）と同様に、ファイルがオープンされた後に該ファイルのデータ（機器固有情報）が格納されるべきデータ部の位置情報ｋが獲得される（Ｓ４１，Ｓ４２）。この獲得された位置情報ｋに基づいて情報C(k)が生成される（Ｓ４３）。この情報C(k)を秘密鍵として用いてデータDATA（機器固有情報）が暗号化され（Ｓ４４）、暗号化データEc(k)(DATA)が該位置情報ｋで特定されるデータ部の領域に書き込まれる（Ｓ４５）。その後、上述したデータ書込時の処理と同様に、全ての情報の書込が完了した後に、ファイルがクローズされる（Ｓ４６）。

【００４７】また、保護されたファイルのデータ（機器固有情報）を記憶装置２０から読み出す場合、コンピュータユニット１０はその読出処理の一部として、図１５

に示すような処理を実行する。この図１５に示す処理の手順が図１７に模式的に示される。

【００４８】この場合、上述したデータ読出時の処理（図１０参照）と同様に、ファイルがオープンされた後に、データが格納されているデータ部の位置情報ｋ’が獲得される（Ｓ５１，Ｓ５２）。この獲得された位置情報ｋ’に基づいて情報C(k’)が生成される（Ｓ５３）。その後、位置情報ｋ’にて特定されるデータ部の領域から暗号化データEc(k’)(DATA)（暗号化された機器固有情報）が読みだされ、その暗号化データEc(k’)(DATA)が上記情報C(k’)を秘密鍵として復合される（Ｓ５４，Ｓ５５）。このように、暗号化データが復合されると、ファイルがクローズされる。

【００４９】もし、上記のようにデータの読出処理において獲得された位置情報ｋ’がデータの書込処理にて獲得された位置情報ｋと同一の場合、暗号化データEc(k’)(DATA)が秘密鍵C(k’)にて正しく復合される。そして、この正しく復合されたデータは正しい機器固有情報として当該ユーザシステム内にて利用される。一方、該ファイルの移動、複写等により両位置情報ｋ’及びｋが異なると、暗号化データEc(k’)(DATA)が秘密鍵C(k’)を用いて正しく復合できない。この場合、正しいデータDATA（機器固有情報）を再び復元することはできない。

【００５０】次に、更に他の処理例を図１６乃至図１９に基づいて説明する。保護すべき機器固有情報に関するファイルを記憶装置２０に格納する場合、コンピュータユニット１０はその格納処理の一部として、図１８に示すような処理を実行する。この図１８に示す処理の手順が図１６に模式的に示される。

【００５１】この場合、上述したデータ書込時の処理（図５、図１４参照）と同様に、ファイルがオープンされた後に該ファイルのデータが格納されるべきデータ部の位置情報ｋが獲得される（Ｓ６１，Ｓ６２）。そして、この獲得された位置情報ｋが付加情報としてデータDATA（機器固有情報）に付加されると共に、該位置情報に基づいて情報C(k)が生成される（Ｓ６３、Ｓ６４）。この情報C(k)を秘密鍵として用いてデータDATA（機器固有情報）と付加情報ｋとが一体となったデータ（DATA+k）が暗号化される（Ｓ６５）。この暗号化データEc(k)(DATA+k)が該位置情報ｋで特定されるデータ部の領域に書き込まれる（Ｓ６６）。その後、上述したデータ書込時の処理と同様に、全ての情報の書込が完了した後に、ファイルがクローズされる（Ｓ６７）。

【００５２】また、保護されたファイルのデータを記憶装置２０から読み出す場合、コンピュータユニット１０はその読出処理の一部として、図１９に示すような処理を実行する。この図１９に示す処理の手順が図１７に模式的に示される。この場合、上述したデータ読出時の処理（図１０、図１５参照）と同様に、ファイルがオープンされた後に、データ（機器固有情報）が格納されているデータ部の位置情報ｋ’が獲得される（Ｓ７１，Ｓ７２）。この獲得された位置情報ｋ’に基づいて情報C(k’)が生成される（Ｓ７３）。その後、位置情報ｋ’にて特定されるデータ部の領域ｋ’から暗号化データEc(k’)(DATA+k)が読みだされ、その暗号化データEc(k’)(DATA+k)が上記情報C(k’)を秘密鍵として復合される（Ｓ７４，Ｓ７５）。復合されがデータ（DATA+k）が位置情報ｋが取り出され（Ｓ７６）、上述した読出処理（図１０参照）と同様に、実際にデータが格納されていた領域の位置情報ｋ’とこの復合にて得られた位置情報ｋとが比較される。そして、それらの位置情報ｋ及びｋ’が同一である場合には、ファイルがクローズされる。

【００５３】ここで、上記両位置情報ｋ’及びｋが同一の場合、暗号化データEc(k’)(DATA+k)が秘密鍵C(k’)にて正しく復合される。そして、復合されたデータ(DATA+k)から分離された正しいデータ（機器固有情報）が当該ユーザシステム内にて利用される。一方、該ファイルの移動、複写等により両位置情報ｋ’及びｋが異なると、エラー信号が出力される。この場合、暗号化データEc(k’)(DATA+k)は秘密鍵C(k’)を用いて正しく復合されておらず、正しいデータDATA（機器固有情報）を再び復元することはできない。　このような処理では、ユーザは、復合されたデータが正しいデータか否かが実際に復合されたデータを使用する前にエラー信号の有無に基づいて判断することができる。

【００５４】上記各情報を格納する記憶装置２０内の領域ｉ，ｊ，ｋは、乱数にも基づいて定められた。しかし一般のシステムでは、所定のアルゴリズムに従って決定される。例えば、通常のファイル操作において先頭から走査して最初に見つかる空き領域が該領域ｉ，ｊ，ｋとして確保される。従って、新しいユーザシステムでは、常に同じ領域が記憶装置２０内に確保されるおそれがある。次に、各ユーザシステムにおいて同一となるデータの書込領域が偶然に確保されることを防止するための他の例を示す。

【００５５】この場合、図２２に示すフローチャートに従って書込時の処理が行われる。図２２において、乱数が発生され（Ｓ８１）、特に意味を持たない一時ファイルがその乱数ｎだけ作成される（Ｓ８２）。そして、この一時ファイルの各情報が、所定の順番にて決定される記憶装置２０内のデータ部、ファイル名管理部及びデータ管理部の各領域に、図２０に示すように、記憶装置２０内に分散して格納される（temp 1, temp 2, ... temp n）。その後、保護すべき機器固有情報に関するファイルが上述したいずれかの処理（図５、図１４、図１８）に従って該所定の順番にて決定される記憶装置２０内の各領域に格納される（Ｓ８３）。その結果、記憶装置２０内は、図２０に示すように、複数の一時ファイルと保護すべきファイルとが混在した状態となる。

【００５６】この状態において、作成したｎ個（乱数）

の一時ファイルを全て記憶装置２０から削除する（Ｓ８４）。その結果、図２１に示すように、記憶装置２０内には、保護されたファイルのみが残る。ファイルの読出時の処理は、該ファイルの格納処理（図５、図１４、図１８）に対応した手順（図１０、図１５、図１９）に従って行われる。

【００５７】上記のように、一時ファイルを格納した後に、保護すべきファイルを格納し、その後に、一時ファイルを削除するようにすれば、各ユーザシステムにおいて偶然的にファイルの書き込む領域が同一となる確率を充分低減させることができる。

【００５８】上記処理例では、一時ファイルの数を乱数にて決定していたが、それに限定されることなく、常に一定の数の一時ファイルを書き込んでもよい。また、一時ファイルの大きさは、全て同じでもよいし、また、乱数等を用いて変えるようにしてもよい。

【００５９】更に、上記各処理例においては、データ部における領域の位置情報ｋをデータDATA（機器固有情報）の付加情報あるいは秘密鍵を作るベースとして用いたが、データ管理部、ファイル名管理部における領域の位置情報ｉまたはｊを、さらに、各位置情報ｉ、ｊ、ｋの任意に組み合わせた情報を付加情報として使用することも可能である。この場合、読出処理において、書込処理に用いられた情報に対応した情報を用いて復合あるいは読みだしたファイルが正当なファイルか否かの判定が行われる。

【００６０】上記各実施例では、保護状態にて販売されるソフトウエアの保護を解除するための鍵（ライセンス）の元となる機器固有情報の保護を行うために本発明を適用したものであるが、他の情報の保護するためにも本発明は適用可能である。

【００６１】

【発明の効果】以上説明したように、本発明によれば、記憶装置から読みだされて復合された情報に該ファイルの書込位置に関する情報が反映される。従って、この情報と実際にファイルを読みだした位置情報との差に基づいて、該ファイルが当該記憶装置に不正に移動または複写されたものかを知ることができる。また、書き込み位置に関する情報と実際にファイルを読みだした位置情報とが一致する場合にのみ、記憶装置に格納されたファイルの情報が正確に復合される。これにより、記録装置に格納されるファイル（パスワード等の秘密情報が保存されるファイル等）が高い安全性をもって保護することができる。

【００６２】更に、このようなファイルの保護システムを用いたソフトウエア利用システムでは、当該システムの固有情報を上記ファイルの保護システムにて保護し、該保護された固有情報を用いてソフトウエアを更に保護している。従って、この固有情報を他のシステムに複写してソフトウエアを不正に利用するという行為が確実に防止される。

【００６３】また、このようなソフトウエア利用システムにソフトウエアを提供する記録媒体には、暗号化されたソフトウエアと共にそのソフトウエアを読みだすために必要な情報が格納され、更に、該ソフトウエア利用システムの記憶装置伊格納すべき固有情報を発生させるために必要な情報が格納されている。従って、暗号化されたソフトウエアが容易に各ソフトウエア利用システムに提供できると共に、特に、該ソフトウエア利用システムに、機体番号等の統一的な固有情報がなくても、この記憶媒体をセットすることにより固有情報がソフト的に生成することが可能となる。

【図面の簡単な説明】

【図１】本発明に係るファイル保護システムが適用されるユーザシステム（ソフトウエア利用システム）の基本構成を示すブロック図である。

【図２】図１に示すシステムに暗号化されたソフトウエア及びシステムソフトウエアを提供するための記録媒体（ＣＤ－ＲＯＭ）を示す図である。

【図３】暗号化されたソフトウエアをシステムにインストールするための手順を示すフローチャートである。

【図４】図２に示す記録媒体に格納されたシステムソフトウエアのインストーラの機能を示す図である。

【図５】機器固有情報を発生して記憶装置に格納する手順を示すフローチャートである。

【図６】記憶装置の論理構造を示す図である。

【図７】記録装置にファイルの情報（機器固有情報）を書き込むための処理の例を模式的に示す図である。

【図８】暗号化されたソフトウエアを復合するために必要な鍵を購入する手順を示すフローチャートである。

【図９】図５に示す処理にて書き込まれたファイルの情報（機器固有情報）を読み出すための処理の例を模式的に示す図である。

【図１０】ファイルの情報（機器固有情報）を読みだすための処理の手順を示すフローチャートである。

【図１１】購入した暗号化された鍵を復合（開錠）する手順を示すフローチャートである。

【図１２】記録装置にファイルの情報を書き込むための処理の他の例を模式的に示す図である。

【図１３】図１２に示す処理にて書き込まれたファイルの情報を読み出すたの処理の例を模式的に示す図である。

【図１４】図１２に示す処理の手順を示すフローチャートである。

【図１５】図１３に示す処理の手順を示すフローチャートである。

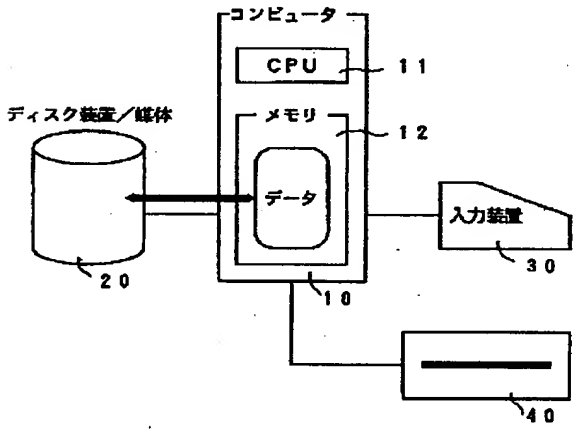
【図１６】記録装置にファイルの情報を書き込むための処理の更に他の例を模式的に示す図である。

【図１７】図１６に示す処理にて書き込まれたファイルの情報を読み出すための処理の例を模式的に示す図であ

る。
【図１８】図１６に示す処理の手順を示すフローチャートである。
【図１９】図１７に示す処理の手順を示すフローチャートである。
【図２０】一時ファイルと保護されるべきファイルの記録装置内における格納状態を示す図である。
【図２１】一時ファイルが記録装置内から除去された状態を示す図である。
【図２２】一時ファイル及び保護されるべきファイルの格納及び一時ファイルの除去に関する処理の手順を示すフローチャートである。
【図２３】ソフトウエアの販売及び利用の形態を示す図である。
【符号の説明】
１０　コンピュータユニット
１１　ＣＰＵ（中央演算処理ユニット）
１２　メモリ
２０　記憶装置
３０　入力装置。
４０　ＣＤ－ＲＯＭドライバ

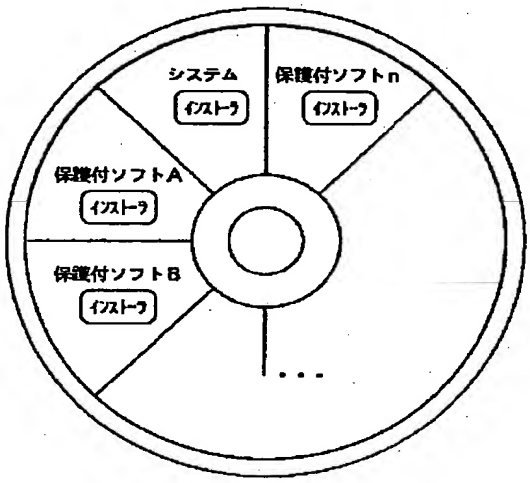
【図１】

本発明に係るファイル保護システムが適用される
ユーザシステムの基本構成を示すブロック図



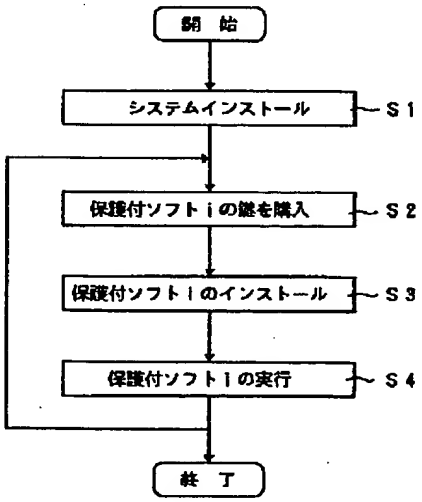
【図２】

図１に示すシステムに暗号化されたソフトウエア及び
システムソフトウエアを提供するための
記録媒体（ＣＤ－ＲＯＭ）を示す図



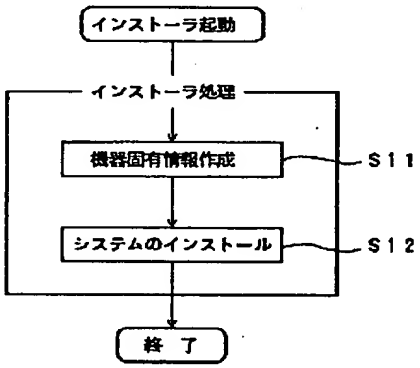
【図３】

暗号化されたソフトウエアをシステムにインストール
するための手順を示すフローチャート



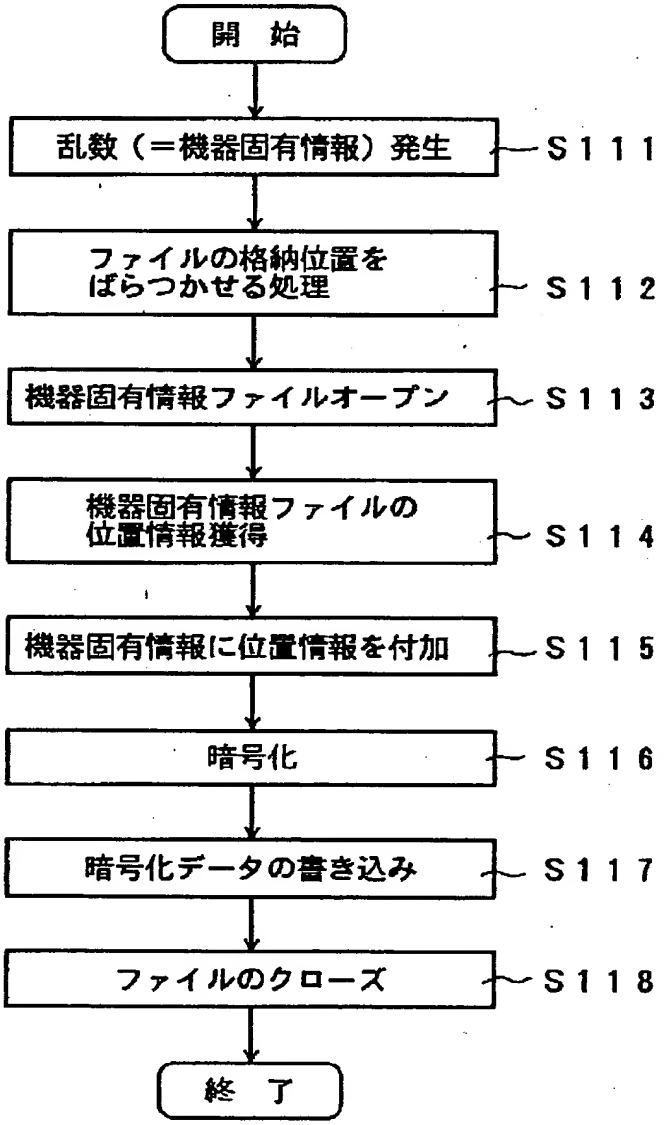
【図４】

図２に示す記録媒体に格納されたシステムソフトウエアの
インストーラの機能を示す図



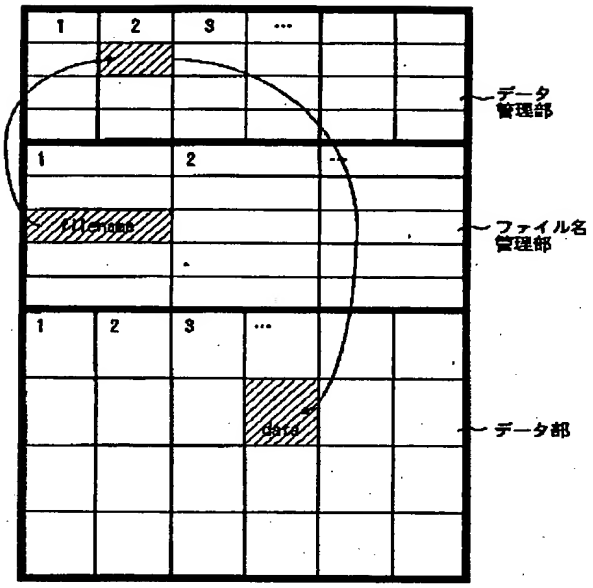
【図５】

機器固有情報を発生して記憶装置に格納する手順を示すフローチャート



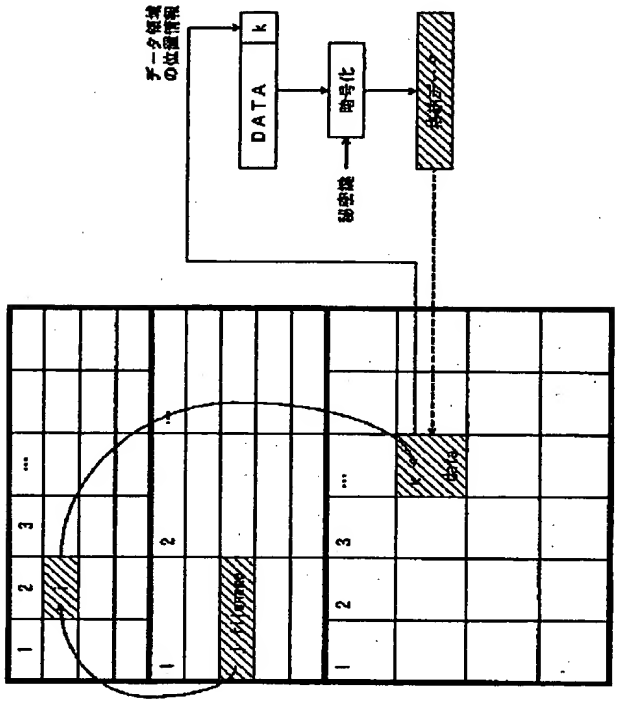
【図６】

記憶装置の論理構造を示す図



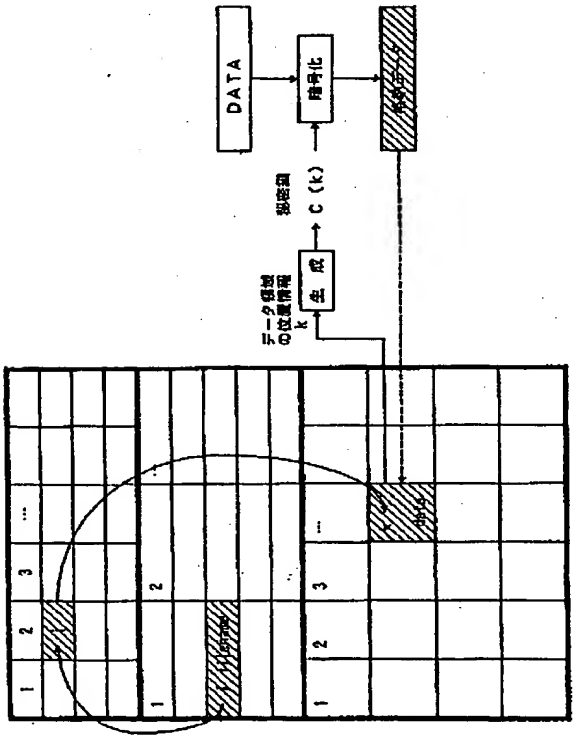
【図７】

記録装置にファイルの情報を書き込むための処理の例を模式的に示す図



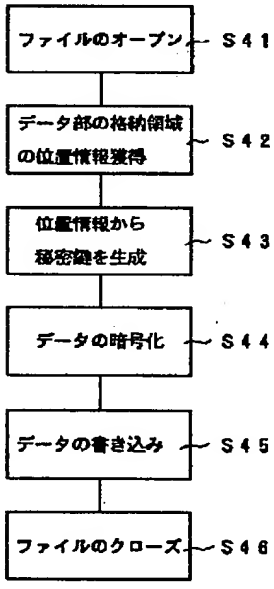
【図１２】

記録装置にファイルの情報を書き込むための処理の他の例を模式的に示す図



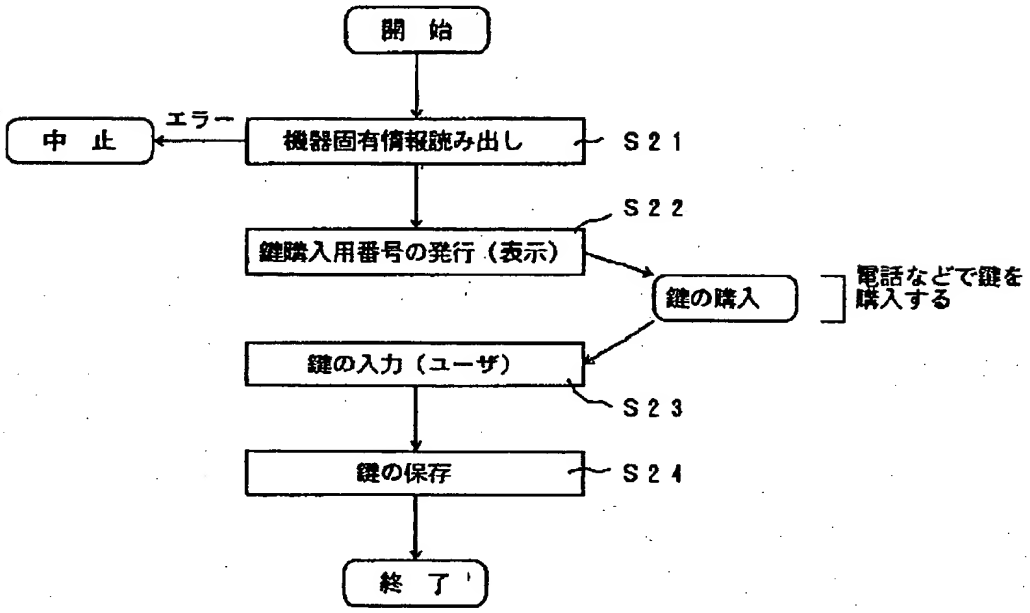
【図１４】

図１２に示す処理の手順を示すフローチャート



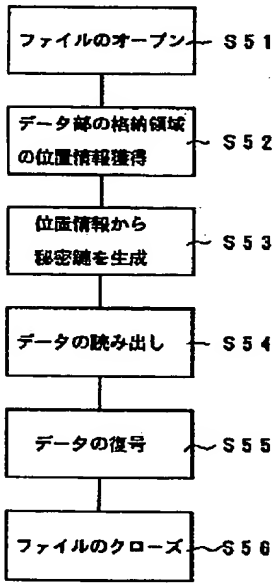
【図８】

暗号化されたソフトウエアを復合するために必要な鍵を購入する手順を示すフローチャート



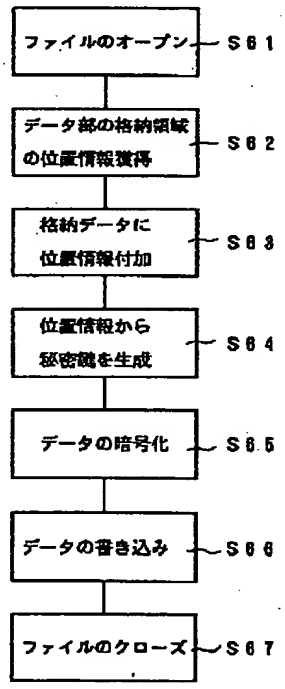
【図１５】

図１３に示す処理の手順を示すフローチャート



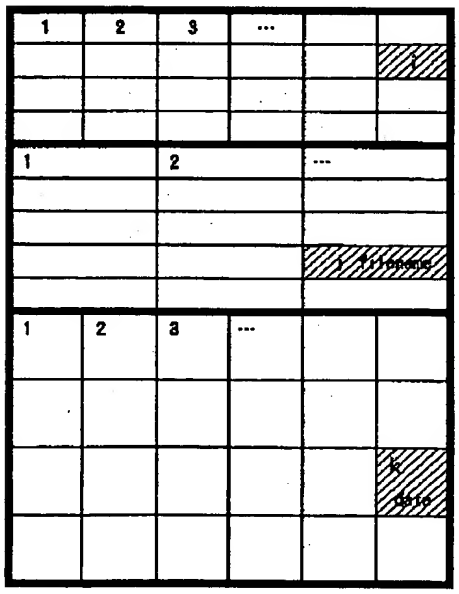
【図１８】

図１６に示す処理の手順を示すフローチャート



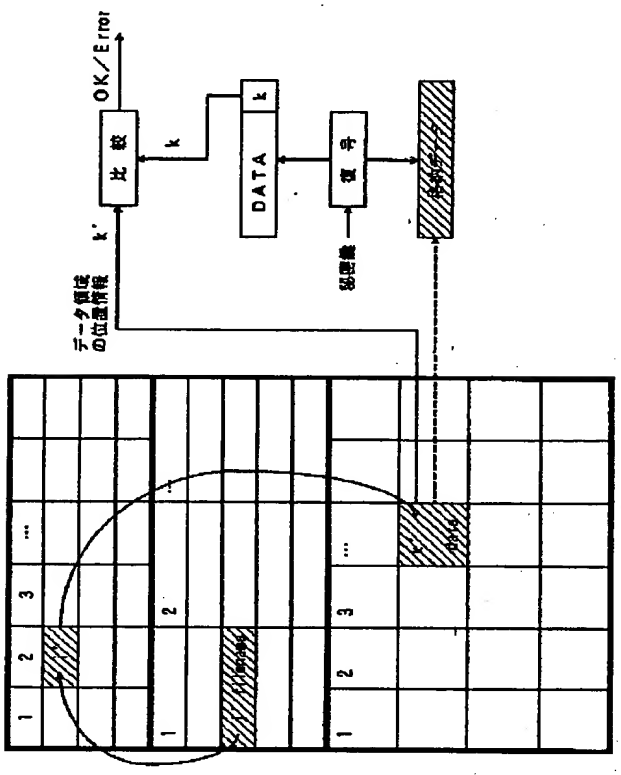
【図２１】

一時ファイルが記録装置内から除去された状態を示す図



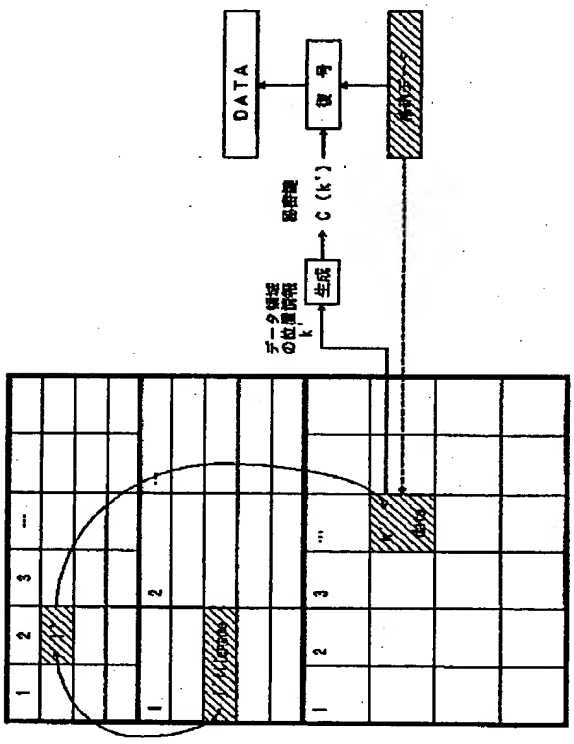
【図９】

図５に示す処理にて書き込まれたファイルの情報を
読み出すための処理の例を模式的に示す図



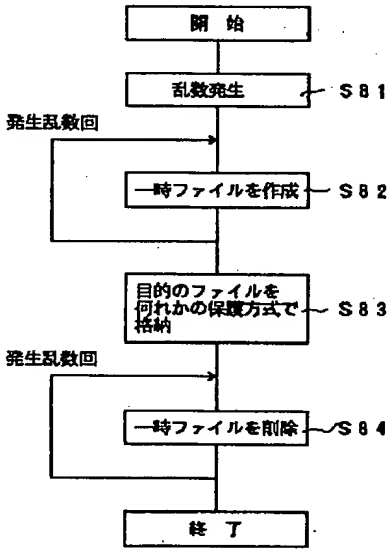
【図１３】

図１２に示す処理にて書き込まれたファイルの情報を
読み出すための処理の例を模式的に示す図



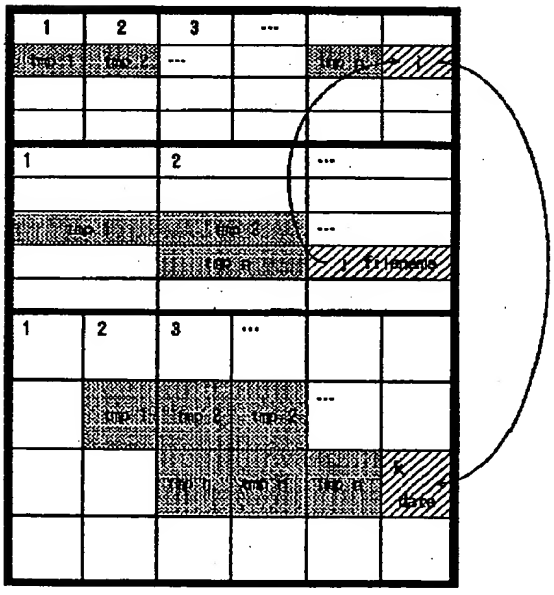
【図２２】

一時ファイルが記録装置内から除去された状態を示す図



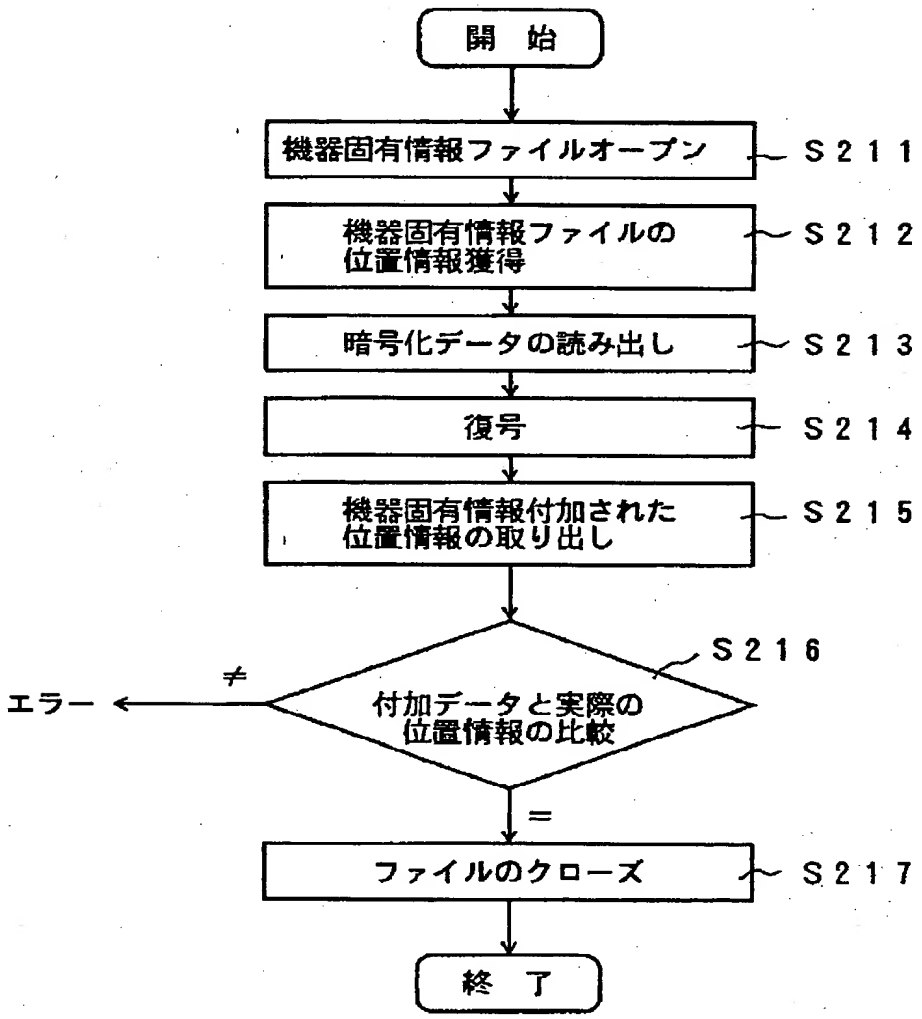
【図２０】

一時ファイルと保護されるべきファイルの
記録装置内における格納状態を示す図



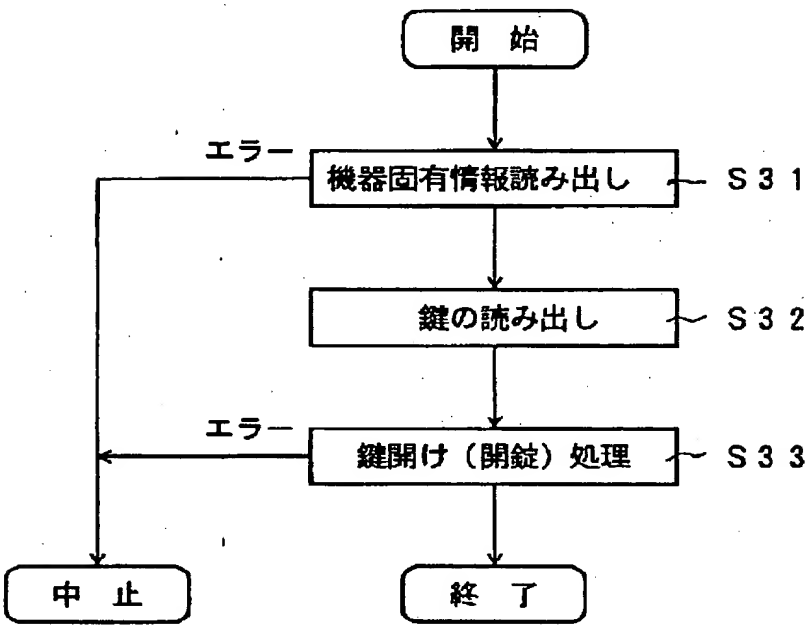
【図１０】

ファイルの情報（機器固有情報）を読みだすための処理の手順を示すフローチャート

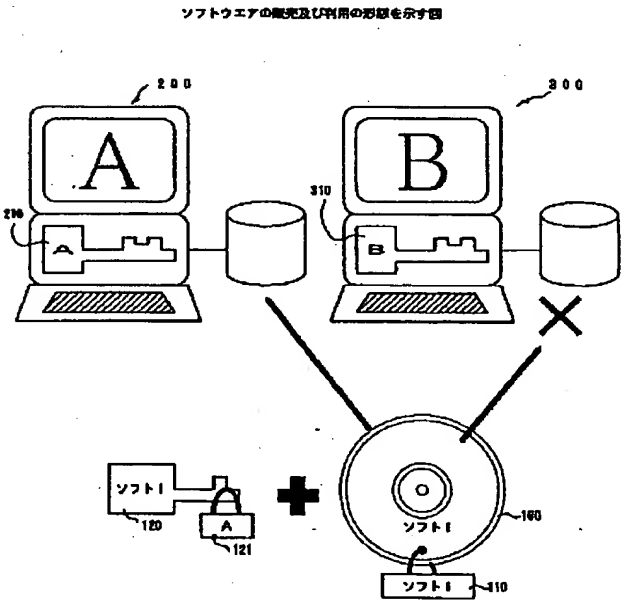


【図１１】

購入した暗号化された鍵を復号化（開錠）する手順を示すフローチャート

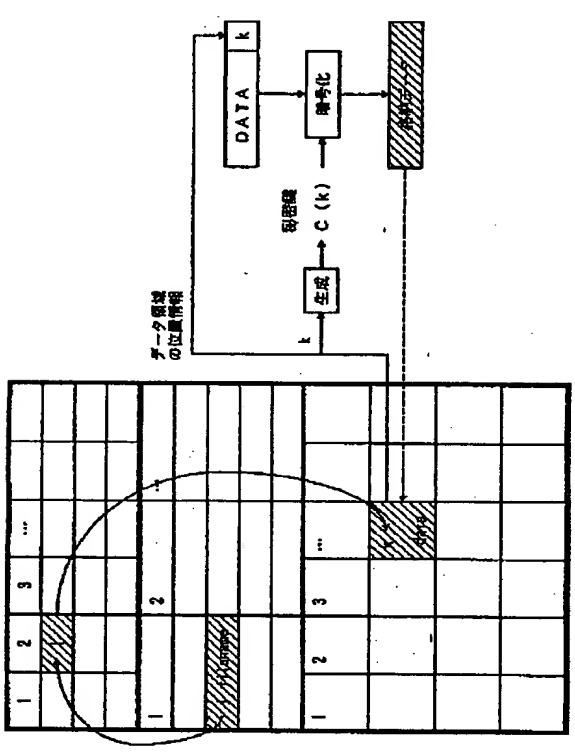


【図２３】



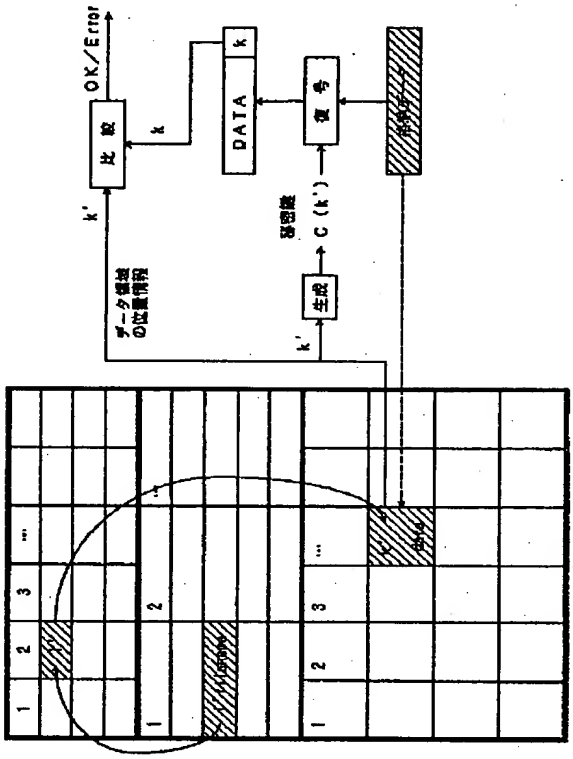
【図１６】

記録装置にファイルの情報を書き込むための処理の更に他の例を模式的に示す図



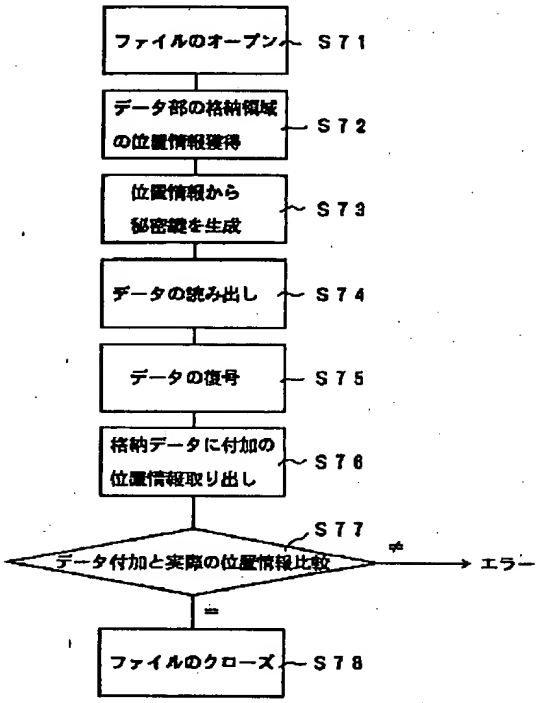
【図１７】

図１６に示す処理にて書き込まれたファイルの情報を読み出すための処理の例を模式的に示す図



【図１９】

図１７に示す処理の手順を示すフローチャート



フロントページの続き

(72)発明者　鳥居　直哉
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　岩山　登
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内